

### **REMARKS**

In the outstanding Office Action, the Examiner rejected claims 1-4 and 6-9 under 35 U.S.C. § 112, first paragraph; and rejected claims 1-4 and 6-9 under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,673,319 to Bellare et al. ("Bellare"). By this amendment, Applicants have amended claims 1 and 6-9. Claims 1-4 and 6-9 remain pending.

Regarding the rejection of claims 1-4 and 6-9 under 35 U.S.C. § 112, first paragraph, Applicants respectfully disagree with the Examiner's assertion "the specification does not disclose 'CBC mode encrypts said data using said set of keys based on at least one of the sectors of said data encrypted by said integrity-check-value-generating key,'" as recited in claims 1 and 6-9. Office Action, page 3.

Initially, the present amendment removes the recitation of "CBC mode encrypts said data using said set of keys based on at least one of the sectors of said data encrypted by said integrity-check-value-generating key" from claims 1 and 6-9. Moreover, Applicants have amended claims 1, 6, and 9, to more clearly define this element. Applicants respectfully submit that the specification at, for example, page 86, and Figure 32, provides adequate support for at least this feature, as recited in claims 1 and 6-9. Accordingly, Applicants respectfully submit that the specification provides support for the subject matter in claims 1-4 and 6-9, and respectfully request that the Examiner withdraw the rejection of claims 1-4 and 6-9 under 35 U.S.C. § 112, first paragraph.

Applicants respectfully traverse the rejection of claims 1-4 and 6-9 under 35 U.S.C. § 102(b)<sup>1</sup>. Bellare, as relied on by the Examiner, cannot properly anticipate claims 1-4 and 6-9. In order to properly anticipate Applicants' claimed invention under 35 U.S.C. §102, each and every element of the claim in issue must be found, "either expressly or inherently described, in a single prior art reference." "The identical invention must be shown in as complete detail as is contained in the . . . claim. *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989)." See M.P.E.P. § 2131 8th Ed. (Rev. 2), May 2004.

Claim 1, for example, recites a combination including "a second set of keys correlated with integrity-check-value generating keys of data to be stored in at least one of the sectors," and "executing encryption processing on the first and second set of keys in a cipher block chaining (CBC) mode using a storage key stored in said data storage device." Bellare fails to teach at least these elements.

Bellare teaches a method of encryption wherein:

[an] encrypting party and the decrypting party share a pair of secret keys (i.e. a first and a second key). At step 70, the plaintext string is cipher block chained using the first (secret) key and a null initialization vector (IV) to generate a CBC message authentication code (MAC) that is the (entire) last block of ciphertext ... the plaintext string is again cipher block chained, now using the second (secret) key and the CBC-MAC ... as the initialization vector, to thereby generate and enciphered string.

---

<sup>1</sup> The Office Action contains a number of statements reflecting characterizations of the related art and the claims. Regardless of whether any such statement is identified herein, Applicants decline to automatically subscribe to any statement of characterization in the Office Action.

Bellare, col. 5, lines 5-16. Bellare, however, is silent as to “integrity-check-value generating keys,” and accordingly fails to teach a combination including “a second set of keys correlated with *integrity-check-value generating keys* to be stored in at least one of the sectors,” and “executing encryption processing on the first and *second set of keys* in a cipher block chaining (CBC) mode using a storage key stored in said data storage device,” as recited in independent claim 1 (emphasis added).

Because Bellare fails to teach each and every element recited in independent claim 1, that reference cannot anticipate independent claim 1. Accordingly, Applicants respectfully submit that independent claim 1 is allowable over Bellare, and claims 2-4 are allowable at least due to their dependence on claim 1.

Claims 6-9, while of different scope, recite elements similar to those recited in independent claim 1. For example, claim 6 recites a combination including “a second set of keys correlating to *integrity-check-value generating keys* of data to be stored in at least one of the sectors,” and “encryption processing is executed on said first and *second set of keys* in the CBC mode using a storage key stored in said data storage device” (emphasis added). Claim 7 recites a combination including “executing encryption processing in the CBC mode using a storage key unique to said data storage device on an *integrity-check-value generating key* of data to be stored in at least one of the sectors” (emphasis added). Claim 8 recites a combination including “executing ... encryption processing in the CBC mode on ... a second set of keys correlated with *integrity-check-value generating keys* of data to be stored in at least one of the sectors, the encryption processing executed using a storage key stored in said

data storage device" (emphasis added). Claim 9 recites a combination including "executing encryption processing in the CBC mode using a storage key unique to said data storage device on an *integrity-check-value generating key* of data to be stored in at least one of the sectors" (emphasis added). For at least the reasons given above with respect to claim 1, most notably that Bellare is silent as to "integrity-check-value generating keys," Applicants submit that claims 6-9 are also allowable over Bellare. Accordingly, Applicants respectfully request that the Examiner withdraw the rejection of claims 1-4 and 6-9 under 35 U.S.C. § 102(b).

Applicants respectfully request that this Amendment under 37 C.F.R. § 1.116 be entered by the Examiner, placing claims 1-4 and 6-9 in condition for allowance. Applicants submit that the proposed amendments of claims 1-4 and 6-9 do not raise new issues or necessitate the undertaking of any additional search of the art by the Examiner, since all of the elements and their relationships claimed were either earlier claimed or inherent in the claims as examined. Therefore, this Amendment should allow for immediate action by the Examiner.

Furthermore, Applicants respectfully point out that the final action by the Examiner presented some new arguments as to the application of the art against Applicant's invention. It is respectfully submitted that the entering of the Amendment would allow the Applicants to reply to the final rejections and place the application in condition for allowance.

Finally, Applicants submit that the entry of the amendment would place the application in better form for appeal, should the Examiner dispute the patentability of the pending claims.


In view of the foregoing remarks, Applicants submit that this claimed invention, as amended, is neither anticipated nor rendered obvious in view of the prior art references cited against this application. Applicants therefore request the entry of this Amendment, the Examiner's reconsideration and reexamination of the application, and the timely allowance of the pending claims.

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,  
GARRETT & DUNNER, L.L.P.

Dated: November 23, 2005

By:   
Darrell D. Kinder, Jr.  
Reg. No. 57,460